한국선급 사이버보안 뉴스레터

2018.05

KR
KOREAN REGISTER

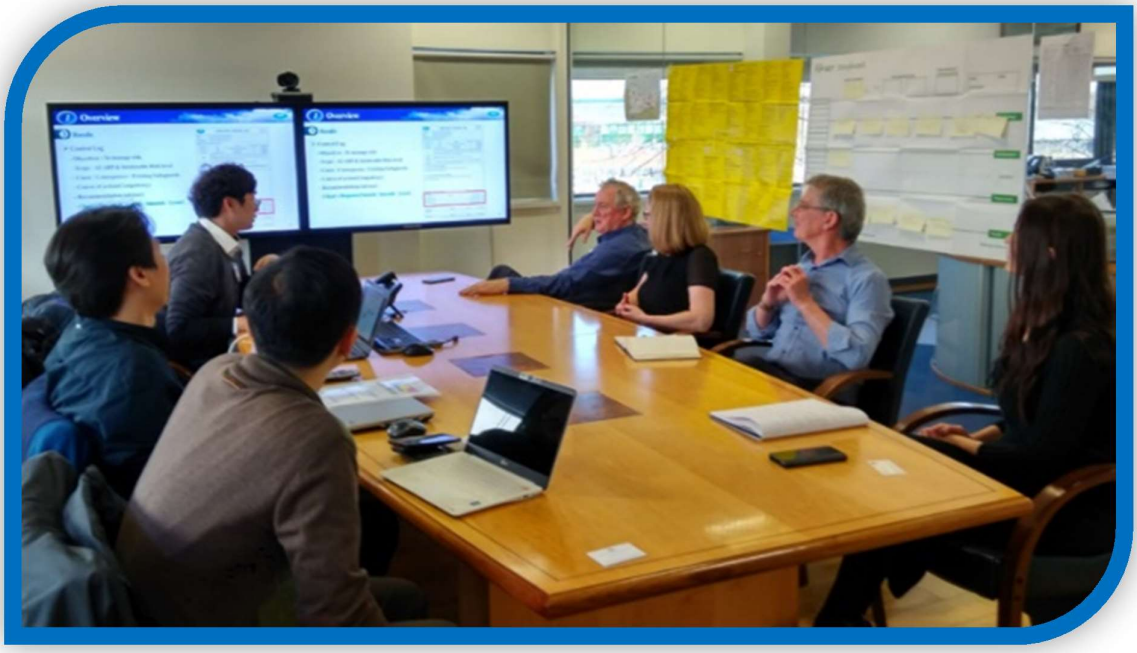
<한국선급 활동>

화주검사 대응 기술컨설팅 수행

KR 은 지난 4 월 영국 글래스고에 위치한 SONGA 선사 TMSA(탱커선 화주검사) 대응을 위한 사이버보안 체계 구축 컨설팅을 진행하였습니다. TMSA Element 13 의 주요 점검항목은 사이버보안 정책 / 절차서에 따른 이행, 사이버보안 리스크평가를 통한 위협식별 및 개선조치, 임직원 인식제고 교육 등으로 선사의 TMSA 수검을 위한 각 점검 항목을 검토하고 이에 필요한 서비스를 제공 하였습니다.

지난 4/28 일 선사에서는 TMSA 수검을 완료 하였으며, 사이버보안 각 검사 항목에 대해서 문제없이 통과하여 선사에서 목표하였던 점수를 달성하였음을 확인 하였습니다.

향후에도 KR 은 지속적인 사이버보안 서비스 제공을 통해 고객만족도 향상에 최선을 다하겠습니다.



사이버보안 관련 최신 정보는 아래의 링크에서 확인 하실 수 있습니다.

http://www.krs.co.kr/sub/kor_board_list.aspx?s_code=0212060200&b_code=004093000

<원격 무인선의 안전 위협 제기>

주요 내용

IMO Maritime Safety Committee 를 앞두고 노틸러스 인터내셔널 (Nautilus International) 이 1,000 여명의 해양 전문가를 대상으로 Autonomous Shipping 의 안전성에 대한 설문조사 결과를 발표하였습니다.

① 응답자 85% 자동화 선박의 위험성 지적

설문조사에 따르면, 응답자의 약 85%는 무인 원격 선박(Unmanned Remotely Controlled Ships)이 해상에서 안전의 위협이 될 것으로 예상하였으며, 선박 자동화가 항해 과정의 위협이 될 것이라고 지적했습니다.

② 기존 전통 선박과 자율 운항 선박간 이슈

노틸러스 인터내셔널 (Nautilus International)은 이번 설문조사와 함께 (International Transport Workers 'Federation), International Federation of Shipmasters 'Association 가 제출한 논문을 근거로 제시했습니다. 해당 논문에서는 자율 운항 선박에 대한 정의가 아직 마련되지 않았고, 자율 운항 선박과 전통적인 선박 간의 상호작용, 사람과 기계(Machine) 간의 인터페이스 이슈(Interface Issue)가 존재하고 있어 보다 많은 주의가 요구된다고 주장하고 있습니다.

③ 사이버보안, 책임 소재 기준 등 필요

IMO MSC 를 통해 이와 같은 내용을 전달할 것이라고 밝힌 Nautilus 는 미래 환경에 대비하여 선박 운항을 위한 이중화와 신뢰성 확보, 사이버 보안, 원격 제어 작업에 대한 책임 소재 등에 대한 문제를 다뤄야 한다고 말했습니다.

대응방안 및 시사점

자율 운항 선박, 무인선 등 ICT 기술을 접목하는 선박의 발전에 발맞춰 시스템의 안전성과 신뢰성을 제고하는 사이버보안 기술이 함께 발전하여야 하며, 기술적인 요소뿐만 아니라

자율 운항 선박 또는 무인선 내 시스템 문제로 인하여 해상 사고가 발생할 경우 그 책임을 어떻게 규정할 것인지도 기준이 필요하다고 판단됩니다.

출처

Unmanned remotely controlled ships pose a threat to safety at sea, May, 2018, Marin Electronics & Communications

<美・英 중국 겨냥 '안보전쟁', 대형통신업체 ZTE 에 제재・경고>

주요 내용

미국과 영국이 잇따라 중국의 대형 통신장비업체 ZTE 에 대해 사이버보안 경고를 발표했습니다.

④ ZTE 에 대한 미국의 추가 제재

미국 상무부는 4 월 16 일 북한과 이란 제재를 위반하고 이들과 거래한 ZTE 에 대해 향후 7 년간 미국 기업과 거래를 할 수 없도록 추가 제재를 부과했다고 전했습니다.

ZTE 는 미국 기업으로부터 구매한 제품 3200 만달러어치를 적법한 승인 절차 없이 이란 기업에 공급한 혐의로 지난해 벌금과 함께 제재 위반에 가담한 ZTE 임직원 해고, 상여금 삭감조치를 부과 받았으나, ZTE 는 상여금을 지급하고, 상무부 조사에서는 허위로 진술했다고 상무부는 설명했습니다.

⑤ ZTE 제품에 대한 영국 사이버보안 당국의 경고

미국의 이번 제재와 함께 영국은 중국 정부가 ZTE 의 통신 인프라에 침투해 사이버 스파이(Cyber Espionage)에 악용될 가능성이 있다고 주장하고 영국 내 통신기업들에게 ZTE 의 장비와 서비스를 이용하지 말라고 경고했습니다.

대응방안 및 시사점

미국과 EU 뿐만 아니라, 중국 역시 '사이버보안법"(网络安全法)'을 2017 년 제정함에 따라 사이버보안은 각 국가별 중요한 의제로 대두되는 실정입니다. 이에 따라 조선소와 선사들은

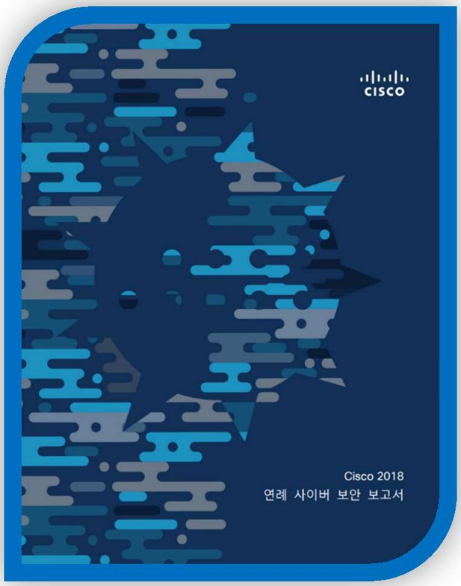
선주 또는 선박의 속한 국가의 사이버보안 관련 법률을 모니터링하는 것은 물론, 필요 시에는 선주와 협의하여 IT 관련 장비 도입 시 위법 요소를 검토하는 것이 필요합니다.

출처

U.S., Britain Issue Warnings Over Chinese Telecom Equipment Maker ZTE, April, 2018, The WALL STREET JOURNAL

<시스코 2018 년 연례 사이버보안 동향보고서 발간>

주요 내용



시스코가 지난 2018 년 4 월 사이버보안 동향을 분석한 연례 보고서(2018 Annual Cyber Security Report) 발간하였습니다. 이번 보고서에서 다루고 있는 내용들은 다음의 세 가지 주제로 요약할 수 있습니다.

① 악성코드의 정교화 파급력 고도화

2017 년 발견된 악성코드 중 랜섬웨어 크립토 웜은 주목해야 할 악성코드로 발표되었습니다. 웜은 네트워크 기반의 악성코드로 일반 악성코드와 달리 자기복제가 가능한 속성을 가지고 있으며, 2001 년 발생한 MS SQL Slammer Worm 처럼 인터넷 전체를 마비시킬 수 있는 잠재력을 지니고 있다고 평가되고 있습니다.

② 사이버 범죄자들이 보안대책 회피능력 증대

기업이 샌드박스(Sand Box) 기반의 악성코드 분석 기술을 향상시킴에 따라 사이버 공격자 역시 샌드박스 환경을 우회할 수 있는 공격수법을 개발하는 데 능숙해지고 있습니다. 예를 들어 악성메일의 첨부파일을 분석하여 특정 샌드박스 우회수법을 사용하는 표본이 급증하다 일순간 표본이 급락하는 경향을 보이는데 이러한 현상은 APT(Advanced Persistent Threat) 공격에 적용되는 대표적인 수법으로 판단됩니다.

③ IoT 보편화에 따른 보안 약점 악용 가능성 확대

IoT(Inter of Thing) 기기가 보편화됨에 따라 사이버공격자 역시 IoT 를 이용하는 봇넷의 활동범위가 증대되고 있는 것으로 조사되고 있습니다. 이런 IoT 기기는 DDoS(Distributed Denial of Service) 공격에 악용될 가능성이 높고 이용자의 기기 사용 가능성에 심각한 위협으로 자리잡게 될 것으로 예상됩니다.

대응방안 및 시사점

최근 사이버공격은 회사 내 일반 임직원이 1 차 공격 대상이 되므로, 임직원이 사용하는 이메일의 첨부파일, 웹 사이트 방문 시 악성코드 감염 가능성에 대하여 지속적인 교육과 인식제고가 필요합니다. 또한 회사 차원의 스팸메일 차단 솔루션 또는 이메일 첨부파일 모니터링 검사와 같은 지속적인 모니터링이 필요합니다.

출처

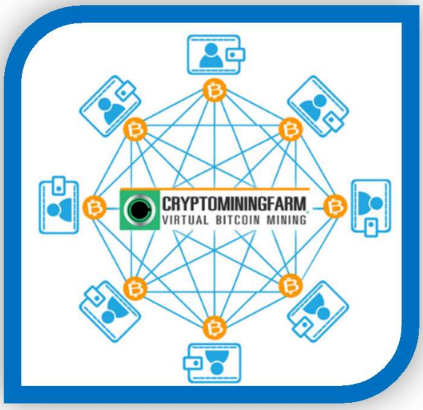
CISCO 2018 Annual Cybersecurity Report, CISCO, April, 2018

<올해 최고의 악성코드 위협, 랜섬웨어가 아닌 크립토마이닝>

주요 내용

코모도 사이버보안 위협 연구소는 2018 년 1/4 분기 악성코드 보고서를 통하여 올해 가장 큰 위협은 랜섬웨어(Ransomware) 기반 공격이 아닌 크립토마이닝(Cryptomining) 기반 공격이라고 전망하였습니다.

① 크립토마이닝(Cryptomining) 공격



용어에서도 알 수 있듯 크립토마이닝 공격은 웹사이트를 방문한 이용자에게 크립토마이너를 설치한 후 해당 PC 리소스를 사용하여 공격자를 위한 가상화폐를 채굴하는 공격 기법으로, 웹 브라우저를 종료한 뒤에도 PC 리소스 사용이 계속 계속됩니다

② 크립토마이닝 공격 증가 원인

이 보고서에 따르면 2018 년 1 분기동안 총 3 억 건의 악성코드 감염 사고 중 약 10%인 2,890 만 건이 크립토마이닝 감염으로 나타났습니다. 악성코드의 변종도 1 월 9 만 3,750 건에서 3 월에는 12 만 7,000 건으로 증가해 빠른 상승세를 보이고 있습니다. 크립토마이너로 급증 이유는 2017 년 이후 랜섬웨어에 대한 기업의 대처 수준이 향상되었다는 점과 높아진 암호화폐의 가치 때문인 것으로 분석되었습니다.

대응방안 및 시사점

사이버공격자는 금전적 목적을 가지고 다양한 공격 수단을 마련하고 있는데 공격 수단은 사회적, 경제적 가치의 변화와 연계되어 지속적인 변화를 모색한다는 것이 특징입니다. 특히 크립토마이닝 공격은 회사가 비용으로 간주하는 전력, 시스템 자원 등을 소모시켜 실질적 피해를 안기는 만큼 사이버 공격에 대한 회사와 선박 내 자원 모니터링에 대한 점검과 관리가 필요합니다. 이를 위하여 회사는 중요 데이터의 악성코드 감염에 대비하여 데이터 백업을 정기적으로 수행하도록 합니다. 또한 백신 업데이트와 악성코드 유입에 대비하여 네트워크 및 시스템에 대한 지속적인 모니터링이 요구됩니다.

출처

Cybersecurity's First Quarter 2018 Threat Report, Comodo, 2018, April

<미국 가스 파이프라인 회사 4 곳 해킹당해>

주요 내용

미국의 천연가스 파이프라인 회사 다수가 해커의 공격을 받았다고 블룸버그 통신이 전했습니다. 보도에 따르면 이들이 고객과 커뮤니케이션 하기 위해 사용하는 전자 시스템이 공격 대상으로 공격 이후 각 가스 파이프라인 회사는 대상 시스템을 폐쇄하는 결정을 내린 것으로 알려졌습니다.

① 사건 개요

미국에서 천연 가스를 수집, 가공, 운송 및 저장하는 회사인 원오크(Oneok Inc.)는 사이버 공격을 받은 사실을 확인한 후 전자 시스템(electronic communications systems) 사용을 중지했다고 발표했으며, 이스턴 쇼어 내추럴 가스 컴퍼니(Eastern Shore Natural Gas Company), 보드워크 파이프라인 파트너(Boardwalk Pipeline Partners LP), 에너지 트랜스퍼 파트너(Energy Transfer Partners LP) 등 4 곳의 미국 천연가스 파이프라인 회사가 해킹 피해를 추가로 보고했습니다.

② 대응

북미 에너지표준위원회(NAESB)에 따르면 이번 공격이 회사가 천연가스 공급을 중단할 정도로 심각한 문제는 아니지만, 각 회사는 해당 전자 시스템 사용을 중단하고 대안을 사용해 통신하고 있다고 전했습니다.

③ 예상원인

지난 달 미국 정부가 러시아 해커들이 전력 회사 및 기타 에너지 회사를 목표로 공격을 조직하고 있다고 경고한 이후 발생한 공격으로 향후 미국 정부의 대응이 주목되고 있습니다.

대응방안 및 시사점

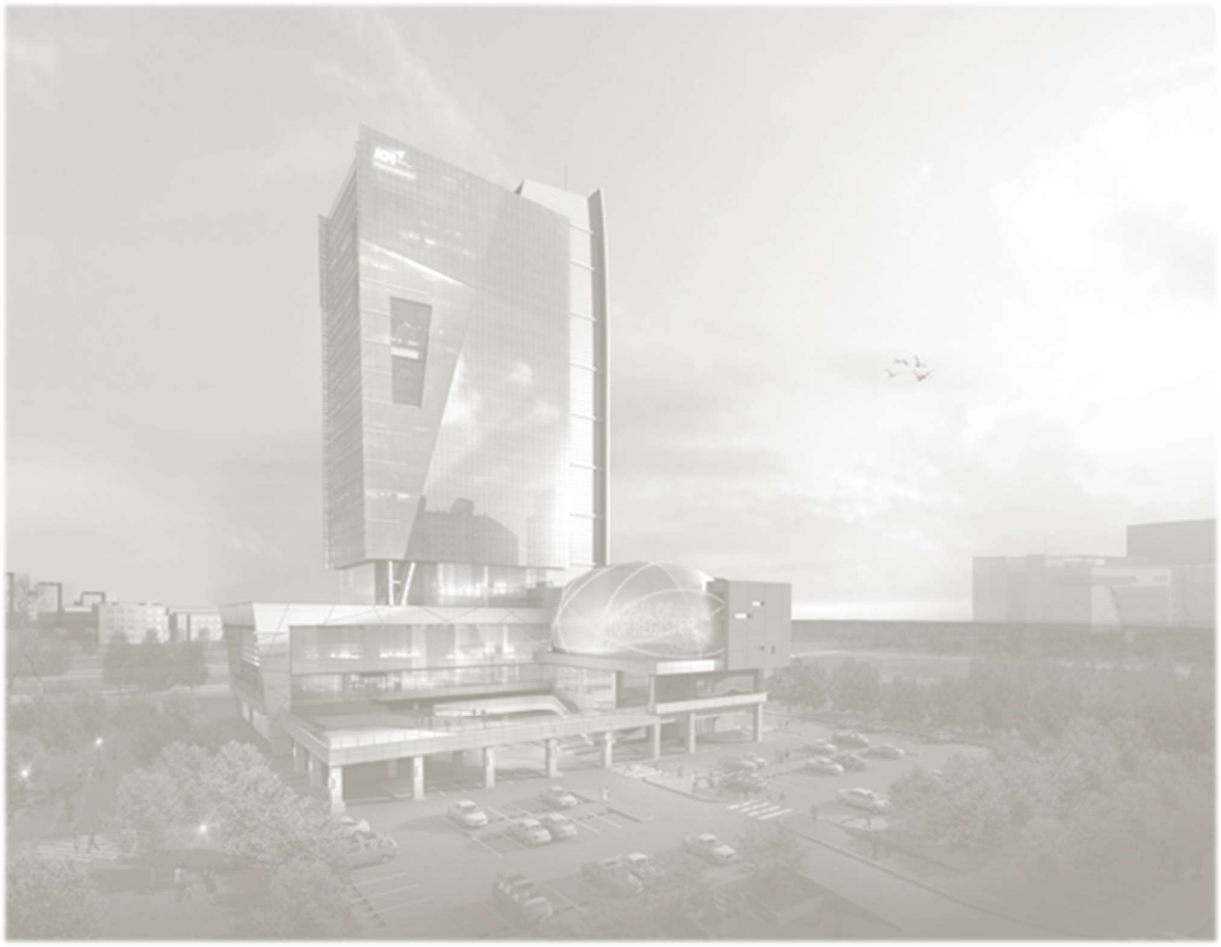
일반적으로 ICS(Industrial Control System)를 운영하는 기업은 사이버공격에 안전하다고 오해하지만 ICS 운영과 관련된 일반 직원의 PC 가 연결됨에 따라 그 위험성은 지속적으로 높아지고 있습니다. 이에 따라 ICS 와 연관된 PC 운영체제 및 SW 의 보안 패치와 백신 운영 확인하도록 하고, ICS 자체의 시스템에 대한 취약점 발표를 모니터링하고 패치를 수행하도록 합니다.

출처

Cyberattack Shows Vulnerability of Gas Pipeline Network, April. 2018, The New York Times

<용어 설명>

- MS SQL Slammer Worm : 악성코드의 일종으로, MS SQL 취약점을 악용하여 버퍼오버플로우 발생시켜 서비스 장애를 유발시켰다. 2003 년 1 월 당시 10 분만에 전세계 75,000 여대 서버를 대상으로 급속도로 퍼져 인터넷 접속이 불가능해졌으며, 특히 한국에서 피해가 가장 컸으며, 2003 년 1 월 25 일 인터넷 대란으로 불린다.
- Sand Box : 샌드박스(sandbox)는 외부로부터 들어온 프로그램이 보호된 영역에서 동작하게 해 시스템이 부정하게 악용되는 분석용 보안 시스템으로 활용되고 있다. 하지만 최근 등장하는 악성코드 중 일부는 자동화된 샌드박스 분석을 우회하도록 설계하여 분석을 피하도록 설계되고 있다.
- IoT(Inter of Thing) : 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술로 이 기술이 탑재된 기기를 IoT 기기라고 지칭한다. 기존에는 상상할 수 없었던 냉장고, 청소기, 가스레인지, 조명, 전력, 가구 등 다양한 가전 기기에 인터넷 연결 기술을 접목시켜 집 외부에서도 이들 기기를 관리 및 통제할 수 있도록 하여 이용자의 편의성을 높이는데 사용하고 있다. 하지만 이런 기기는 보안성이 낮아 사이버공격의 취약 분야로 지목되고 있다.
- 랜섬웨어(Ransomware) : 몸값(Ransome) + Software 의 합성어로 악성코드를 감염시켜 시스템 접근을 제한하고 몸값을 요구하는 악성코드를 지칭한다. 일반적으로 사용자 PC 나 서버가 랜섬웨어 감염되면 악성코드를 풀 수 있는 암호키를 입력하지 않으며 데이터 접근이나 시스템 사용이 불가능 하게 된다. 사이버공격자는 암호키를 담보로 이용자들에게 비트코인 등을 요구함으로써 금전적 이익을 취하게 된다.
- ICS(Industrial Control System) : ICS 는 선박은 물론, 공장, 발전소, 가스, 교통 등 생활 전반에서 사용되는 시스템을 통칭하는 용어로, 일반적으로 다양한 센서(Sensors)와 PLCs(Programmable Logic Controllers), SCADA(Supervisory Control and Data Acquisition) 등으로 구성되어 있다. 과거에는 ICS 가 인터넷 환경과 분리되어 사이버공격의 노출이 거의 없었으나 최근에는 관리의 편의성 등을 목적으로 별도의 관리용 시스템이 인터넷으로 연결되어 사용됨에 따라 사이버공격에 노출될 가능성이 높아지고 있다.



End Document

2018-05-16